Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1846 12/09/16

~ Chrome To Issue Warning ~ People Are Talking! ~ Firebee News Update!
~ AtariCrypt Collection! ~ Fan Castlevania Killed? ~ Twitter Has Accident!
~ DDoS Targets Warcraft! ~ Nintendo’s Bug Bounty! ~ Facebook Struggle?

~ RetroEngine Sigma Mini! ~ ~ TurboGrafx Trademark!

-* The FireBee: The Modern Atari *-
-* EU Vows To Combat Online Hate Speech *-
-* Obama’s Got A New Cybersecurity Plan, So? *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

While there’s little visible in my area to show that winter is here, a step outside will deinitely prove that we’re in the midst of the chilly seaon! Arctic cold is rapidly approaching, dropping temps to the lowest they’ve been this year! I’m not looking forward to this weekend in that regard!

The holiday season is in full gear. The Salvation Army bell-ringers are out in full force; holiday music is blasting away on every mall Muzak machine; decorations abound in stoers and neighborhoods; and letters are headed in earnest to the North Pole! Here at home, we are looking ahead to a very quiet holiday season this year; our main focus is on our construction project - razing our current house in order to re-build and add on. Packing and storage is definitely not one of most favorite pasttimes!

As mentioned a few weeks ago, we’re winding down our work here at A-ONE. It’s highly doubtful that we’ll see an issue in 2017; I’ll likely put together our last issue within the next couple of weeks. I have to say that I appreciate everyone’s support over the years, especially you, our long-time and faithful readers. Without your kindness over the years, we would not have stood the test of time and patience. So, thank you!

Until next time...

=~=~=~=

The FireBee: Modern Atari Clone

The FireBee is a new Atari-compatible computer. Ataris and Atari-Clones are special computers with their own hard & software. They aren’t PC’s, Mac’s nor Amiga compatible.

A FireBee is similar to an Atari Falcon and works very much like that. It will run most of the Atari compatible software that would run on a Falcon. Different to older Ataris and their clones, the FireBee is a modern computer that supports almost everything you’d expect from a today’s machine, like USB ports, Ethernet,

DVI-I monitor connector, SD-card reader and more.

This brand-new Atari compatible is not cheap, but much like the current Amiga computers, if you're worried about the price, you're probably not the intended audience. Note that even though the order page says "pre-order", I think that's a typo - you can order them directly from the Swiss company that makes them, too.

I love that people and companies are passionate enough to keep developing, building, and selling machines like this - it's a vital effort to keep platforms alive well into the future.

FireBee New Update

Full-length Report About The Level Shifter Problem

What follows is the detailled background report about the killjoy of this summer...

It all began with the fact that most of the finished boards wouldn't even start, after they had arrived at Medusa. The few that did consumed so much power that they caused the generously sized power supplies to fail. We don't want to bore you now with the details of how we located the problem and debugged the hardware, but instead skip to the description of the actual problem. After many tests it appeared (and was later confirmed) that the issue was with the level shifters of the FireBee. These 6 level shifters per board (positions U25 and U31 to U35) are small chips that convert the power and create all the special voltages that are needed by the various different ICs, e.g. 3.3 Volt, 1.45 Volt, 1.8 Volt etc. These are directional 8-path voltage converters from Texas Instruments. It is a "standard" model: 74LVC(8T)245. It's needed because back in the Atari days, 5V were the standard voltage in computers, but the more modern FireBee electronics use 3.3V (or, as mentioned, even lower voltages). The casing we use is an "QFN" (Quad Flatpack No leads, 4-side casing without legs) with an exposed pad, i.e. a metal surface on the lower side. This was supposed to be used as a "Thermal Pad", in order to improve the cooling of the ICs through the circuit board.

These so-called "Thermal Pads" therefore have to be soldered onto the board completely flat in order to properly dissipate the heat generated when converting the voltage. The schematics of this IC (also called "level converter") from Texas Instrument does not show any electric connection of the lower surface of the "exposed thermal pad" with any other structure on, or inside, the chip. The specification only states that the thermal pad "must" be soldered on. For this reason, the FireBee was designed to use the 3.3V part for the cooling. An unconventional and really pretty innovative idea that would help save resources and space on the curcuit board. The prototypes also confirmed that this worked fine. The "conservative" approach would have been to solder the "thermal pads" of these six voltage converters on GND.

What happened with the second batch is that the resistance of the level converters started to change during operation. When new,

the resistance between the "exposed thermal pad" and GND is infinite. When the parts were soldered off and brand-new ones were bought by MCS and used for verification, resistance was a few KiloOhm while running at 25°C. When the temperature rose to a 100°C, the level fell to a few hundred Ohm. Sometimes the bus-drivers heated up to over a 110°C... kind of a vicious circle, really: directly after switching on the computer, the board started to change. The warmer it got, the lower the resistance was, and the more power would flow, and it would heat up even more.

So without any external influence, the behavior of the computers changed under load. You can probably imagine what that meant for the first few weeks of debugging the hardware. A system with almost 1000 parts on an 8-level multilayer board, which had been proven to work fine, and on which nothing had been changed, but still suddenly started to do what it wanted and behave differently every few seconds. In retrospect, that was a great episode from the E-tech horror shop... but in July, without any idea what the problem was, not funny at all!

The final assumption on our side is that TI changed the "diebond material" (glue in the chip) in their IC production, which is used to connect the IC-structure with the thermal pad internally. Some of these glues can become conductive when heated. Unfortunately, we could only get a brief statement from TI about the thermal pad supposedly still "not being connected internally".

The problem clearly lies with TI. The company has changed the physical properties of the ICs somehow, and at some point in time, but not documented these changes anywhere. Until today, and despite intensive searches for PCNs (Product Change Notes) on various channels, we were unable to find any information about it. So the current chip is, officially, exactly the same as in the previous batches - but it is objectively not true. We were also unable to find out when exactly the changes occurred - with which new chip series, or in which production period.

A hardware developer who joined the discussion during the analysis and offered his help, put it this way: "MCS has worked to the best of their knowledge and should IMHO not be the ones paying up for the costs". All of this also explains why the assembly company is also not to be blamed for this whole misery. Despite our announcement to fix the problem free of charge, costs of almost 3000 Euro have been amassed. The reason being that the assembly company now has to remove the six bus-drivers, glue some isolating but heat-dissipating Kapton tape on the lower surface of the thermal pads, and then has to solder them back on - all of this for a 3-digit number of boards. And all of this despite the fact that they also did nothing wrong and caused no production problems at all. Anyone who is familiar with motherboard production knows that this custom fixing process, for such a large number of boards, and at that price, is absolutely amazing! Our assembly company also has been very forthcoming and supportive during the search for the cause of the problems, and when communicating with the vendors and manufacturers. A great service, and an exemplary collaboration!

We hope that this explains why we are asking you for donations.

We, as a project, don’t want that one single person who already had invested a lot of their spare time to make the FireBees available at the production cost of the hardware, now has to pay up for all the costs. On the other hand, we also don’t want to raise the price of the boards, since you pre-ordered them at a specific price. And the assembly company has no fault in any of this, as described before. Finally, any attempt to try to get money from a large semiconductor manufacturer due to problems caused by their faulty documentation - even though the first batch and the prototypes behaved completely differently - is obviously futile. So, for all these reasons, we would again ask you kindly to show solidarity and to foot up the bill together.

Thanks also again for all the trust you have put in Medusa, and the support you gave us during the delivery delays and problem analysis!

Donations please as described either by PayPal to

mcs (at) kingx (dot) com

or by wire transfer to:

MCS Aschwanden
Buchhaldenstr.16
8610 Uster
Switzerland
Bank account Nr.: 202-805498.40F
IBAN: CH22 0020 2202 8054 9840 F
BIC: UBSWCHZH80A
"reason for payment": FB series 2 donation

AtariCrypt Collection Volume One - Merry XMAS! Folks

Greeting Atarians, my great Colleague Steve Gregory a.k.a. Ataricrypt has joined forces with me to bring you the Atari ST Scene a very special gift this 2016 xmas :).

I present to you "AtariCrypt Collection Volume One"

In this "FREE" digital magazine with will find over 70 pages of amazing content personally selected from the AtariCrypt Archive by Steve himself, where I come in as the Suit Taylor to dress it up.

The Magazine covers some of the best Atari ST games as well as some great interviews thrown in for your enjoyment, and with AtariCrypt and Greyfox massive fans of the Atari ST Demoscene, well we just had to include an entire section dedicated to the Demoscene of the present, so please do check that out too. :)

You may direct view the press release and download link here:
https://ataricrypt.blogspot.com/2016/12/ataricrypt-magazine.html

So I hope you all will enjoy the labour of our love and that your nostalgic juices and love for the Atari ST will go wild

this Xmas.

Merry Xmas everyone

the ST Army of Two

Steve Gregory (Ataricrypt) & Darren Doyle (Greyfox)

=~=~=~=

->In This Week's Gaming Section - DDoS Attacks Target Warcraft, Overwatch Again !
"""""""""""""""""""""""""""""""" Nintendo Targets 3DS Vulnerabilities in New Bug Bounty
Konami Kills Fan Castlevania Unreal Based Remaster!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

DDoS Attacks Target Warcraft, Overwatch Again

Blizzard s servers have been affected by DDoS-caused outages multiple times over recent months.

Miscreants have struck Blizzard servers again with multiple waves of DDoS attacks over the last 12 hours. Warcraft and Overwatch, two massively popular games, have been facing latency, login and disconnection issues even while Blizzard has been working on fixing the problem.

The company first acknowledged the problem in a tweet Sunday evening.

Since then, Blizzard claimed to have regained control over matters at its end, only to announce twice the DDoS attacks had restarted. Its last update, at 11:42 p.m. EST Sunday, came three hours after the last wave of DDoS attacks.

On Twitter, a group calling itself Phantom Squad claimed responsibility for the attack.

Blizzard also provided a link to a support page on its website that may help some users troubleshoot their connection problems.

As always, social media was abuzz with users venting their

frustration at the gaming servers being affected. This is at least the fifth such instance in the last few months.

Nintendo Targets 3DS Vulnerabilities in New Bug Bounty

Nintendo has announced it s now supporting a bug bounty program for researchers to find flaws in its 3DS family of handheld game consoles. Researchers could make up to $20,000 for discovering vulnerabilities for the 3DS that could be used for pirating games, enabling cheats, or distributing inappropriate content to children .

Nintendo s 3DS is the latest incarnation in a series of handheld consoles from the manufacture over the years. The 3DS consoles have internet connectivity, which is intended to help gamers shop for new games, connect with other friends using the 3DS, and surf online with a built-in browser.

And where there s internet connectivity there s an attack vector, right? Though the internet connection may seem like a no-brainer target for the bug bounty, most of what Nintendo is focusing on is actually hardware-based. Specifically, they re targeting system vulnerabilities in the ARM9 and ARM11 chipsets, which ship with various versions of the 3DS since the console s initial release in 2011. These vulnerabilities are generally exploited via software loaded directly to the console by SD card.

These are vulnerabilities Nintendo is especially interested in, according to its new bug bounty page:

- System vulnerabilities regarding the Nintendo 3DS family of systems
  - Privilege escalation on ARM11 userland
  - ARM11 kernel takeover
  - ARM9 userland takeover
  - ARM9 kernel takeover
- Vulnerabilities regarding Nintendo-published applications for the Nintendo 3DS family of systems
  - ARM11 userland takeover
- Hardware vulnerabilities regarding the Nintendo 3DS family of systems
  - Low-cost cloning
  - Security key detection via information leaks

Like Apple, Nintendo takes a walled garden approach to the software you are allowed to run on its hardware. If Nintendo users want to run software that Nintendo hasn t specifically approved, they have to get creative. On iPhones, breaking out of the walled garden is called jailbreaking; on Nintendos, it s known as modding, using security holes to modify the 3DS s core software to remove the restrictions that limit the device to approved software only.

That s why vulnerabilities in the ARM9 and ARM11 chipsets are like gold dust to modders: security holes in the CPU itself can often be exploited to bypass the security checks inside the Nintendo operating system itself.

Mods that bypass Nintendo s checks can be used for editing a game s save files (in a word, cheating) and dumping unlawful copies of game software (in a word, piracy), but they can also be used for running software not written by Nintendo, such as open-source games and system emulators. In other cases, modders are simply working to fix what they see as bugs or gaps in a specific game s functionality in effect, providing their own patches.

Of course, if security researchers heed the call of the bug bounty, then at least some of the holes they find will allow Nintendo to close holes currently used for 3DS modding.

On the other hand, exploitable security holes are a cybercriminal s dream, too, so the sooner they re found by the Good Guys, the better.

Konami Kills Fan Castlevania Unreal Based Remaster

It is not all that often that we write something negative about Konami. I prefer to make jabs at them for ignoring fans and letting TONS of great intellectual properties just sit and rot. Well, this article is different, almost in between poking the sleeping giant and pointing out a ray of hope for fans. This is going to be confusing to say the least. For now, the fan remaster of Castlevania using the Unreal engine is dead thanks to a cease and desist from Konami. That is not where the story ends though. There is a faint light at the end of this tunnel.

We wrote up the fan based remaster of Castlevania using the Unreal engine back in October. At the time it seemed like the amazing remake was going full steam ahead and was, well, making Konami look boring. At least the official releases in the Castlevania line. This may be what spurred Konami into action against the fan remake. Can t have fans showing up the intellectual property owner now can we?

Originally released about 30 years ago, Castlevania has been a staple on every console that it has appeared. This game singlehandedly helped make Konami a household name (I really liked Castlevania II: Simon s Quest on the Nintendo Entertainment System).

What is unique about this C&D is that Konami is letting Dejawolf keep the files up. For now, that is. They are not requiring the files be removed, like Nintendo has done in their C&D requests. Just work has to cease immediately. Not too hard to abide by.

What is the glimmer of hope in this story? Well, a member of Konami UK is working on helping Dejawolf to get an official license to use the Castlevania properties. How cool would it be to see Konami open the doors to fans, that can afford it, to license classic IP s? Could we see a fan remake of Bonk s Adventure? Could Adventure Island be far behind if that was to happen?

I know from personal experience that Konami is open to licensing their IP s out but they will do no work other than verification of quality and such in relation. This could become an officially licensed game.

Konami Files New Trademark for TurboGrafx

Konami filed a trademark for TurboGrafx with the United States Patent and Trademark Office. The trademark covers a broad group of classifications pertaining to video games and video gaming consoles.

The filing, discovered by NeoGAF user Rösti, was filed December 1. The application has merely been filed at this point, however. The filing is currently "awaiting examination" by the USPTO.

For those unaware, TurboGrafx-16 was a console created by NEC and Hudson Soft in the late ’80s, sold in Japan under the name PC Engine.

While the TurboGrafx-16 failed to excite consumers outside of Japan, it was notable for being the first home console to have a CD-ROM add-on. Additionally, the TurboExpress was a fully-portable version of the home console, and one of the coolest handhelds ever created.

The trademark filing is broad in scope, so it’s hard to nail down what exactly Konami might have planned for the trademark. As Rösti notes in the original NeoGAF post, Konami controls the IP of Hudson Soft, creators of such titles as Bomberman, Bonk’s Adventure, and the Adventure Island series, so there’s that. Which is nice.

Whatever Konami has in store for the TurboGrafx trademark, it can’t possibly be as heartbreaking as the Metal Gear Solid 3 pachinko machine.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

IndieGoGo RetroEngine Sigma Mini Console and Media Player

Remember the success of the Ouya? It was a Kickstarter success story that people like me are still bringing up. It was that big of a deal. At least the Kickstarter side of things was a big deal, after launch not so much. RetroEngine Sigma is looking to do something similar but not as ambitious as the Ouya did. Think more classic focused with a smattering of video consumption on

the side and you have a good idea of what the RetroEngine Sigma is about.

First of all, the RetroEngine Sigma is nothing more than an emulation machine with Kodi installed. Both of these are often mistaken as illegal options they are not themselves illegal though what you do with them may be so keep that in mind. The Kickstarter is already funded by a few times over and this campaign still has a good month to go. I am not here to sway anyone to not invest in this if this is what you are wanting for your media center (I admit the case is very nostalgic and cool to me).

The RetroEngine Sigma is allegedly capable of playing everything from the Atari 2600 to the Sega Genesis/32X and Sony Playstation (the first one, the PSOne). You will have to supply the games that you wish to play on these emulators (and surely the BIOS files of some like the PSOne as well). While there are legally free ROMs available, there are no legally available BIOS files (to do it legally you will have to go through quite the process).

The RetroEngine Sigma is housed in a case that greatly resembles the Sega Genesis. I so wish there was options to get cases in the style of the Super Nintendo, Playstation One console, or the Neo Geo. Those are iconic systems too. Oh well, can t have everything. Each unit is equipped with HDMI out, two USB ports and a Micro USB port for adding more USB ports. You can go wireless with a USB Bluetooth dongle too.

They have not stopped there. If you so desire you can run the RetroEngine Sigma as a full blown desktop. While the device will apparently feature a quad core CPU, that does not mean it is going to be a satisfying experience as a computer so be warned there if that is your main buying point.

I almost forgot to mention this bad boy supports 4K video.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Obama’s Got A New Cybersecurity Plan, But What’s The Point?

There’s been a lot of hot air blown across headlines this week about the big cybersecurity plan proposed by the White House’s Commission on Enhancing National Cybersecurity (PDF).

The plan for a commission to create long-term recommendations on beefing up America’s cybersecurity was first hatched in April. It’s a roadmap that should’ve been plotted many years ago, and is now being re-gifted to the next administration. Which may or

may not use it for toilet paper.

The report, which identified six key issues for improving the cybersecurity of the US as a whole, is meaningless without the buy-in of the next administration. "The Commission considers this report a direct memo to the next President," it states. "It is critical that the next President and his Administration and Congress begin immediately to tackle each one of the issues raised."

Seeing the report put in motion by the next administration and Congress would be a good thing, if it happens in some form or another. That's because the report nails it when identifying problems, like securing Internet of Things (IoT) products ASAP. The report finally policy-izes fixing things people like me have been raising the alarm about for years. Namely, that the tech industry rushes things to market before securing them, that organizations no longer have control over people, devices, and data, and that attackers are cashing in on our security fatigue.

Sounds good, right? It also includes a generous amount of attention to consumer rights, even suggesting a security "nutritional label" to help citizens assess the risks of products before they buy. Instead of telling us how many calories are in bran flakes, they want us to look at tech products and see "a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand."

There is a fair amount of hate in the report for the traditional username/password system everything runs on for login security. This translated into the Commission's hardcore fanboying of the FIDO Alliance, whose emphasis is on getting rid of the traditional password model in favor of multifactor, biometrics, and items like YubiKey.

I'll even give the report bonus points for mentioning the Mirai attack in its intro -- the concerns presented are up to date. Most reports and the cyber plans of would-be presidents are basically, "internet is dangerous because Target got hacked in 2013." I'm not joking.

However, most of the news this week omitted the fact that the 100-page report, based on nine months of study, has a few spots of rot under its shine.

The Commission behind the report was comprised of 12 members that included corporate interests like the President and CEO of MasterCard, the corporate VP from Microsoft Research, the Chief Security Officer of Uber (Joe Sullivan, formerly Facebook counsel), and former NSA head General Keith Alexander. Some of you may remember Alexander as the NSA's "collect it all" guy, and who was forced to admit that the number of terrorist plots foiled by blanket surveillance were wildly and inaccurately overstated.

While I agree with the report's call to have the private sector and government collaborate on a cyber roadmap, and for that map to espouse citizens' rights, if their idea of private sector means Uber, there's a problem. You know, the same Uber that just decided to track its iOS users even when the app is turned off,

bypassing the iPhone’s consumer-protecting anti-tracking settings.

The Commission’s twelve "subject matter experts" didn’t come from the sprawling cybersecurity industry itself, who are out there in the trenches, over which this policy will govern. Instead, the Commission tapped NIST, DHS, DoJ, DoD and GSA - to ensure the apple doesn’t fall too far from the tree, we must suppose. I mean, yay NIST. But seriously: where was the actual public sector when these guys were in the pillow fort writing fanfic about making passwords go away?

Some sections seem a little less on the level in terms of fighting the good fight for us little people.

There’s quite a bit about protecting companies from being responsible for anything if they cooperate with the government on information sharing. Because I guess CISA just wasn’t enough. Action item 1.2.3 is about public-private sharing of "risk management practices" (like the actions of an organization’s security team, etc) under the banner of security. This would explicitly protect companies from FOIA, discovery in litigation, use in regulatory enforcement, use as evidence, etc... Hey, maybe that’s one of the recommendations we can thank Uber for.

Another curious section talks about working with the international community on "harmonizing" standards and policies, all in an envelope of securing the digital economy. A sagacious person implementing this might explore how it plays out with repressive regimes who could do a lot of damage under the guise of "incident response." Like when China and Russia made moves in 2012 to pass an international treaty that would allow UN member states to cut off and potentially intercept communications under vague wordings for cases that, "appear dangerous to the security of the State [...] or to public order or decency."

Ultimately, the report’s results are a range of recommendations as action items that direct the next president to create initiatives, carve out budgets, make Executive Orders, and collaborate extensively with the public sector. It states that within the first 180 days of the next administration, "the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices."

The report urgently expresses the need for funds to get federal organizations like the old hacked-to-the-gills OPM up to speed with security. "The next President should formally announce his intention to increase investment in modernizing federal IT," the Commission wrote. Based on a calamitous shortage of cyber-workers, the report urges the next President to "initiate a national cybersecurity workforce program to train 100,000 new cybersecurity practitioners by 2020."

President Obama has made it crystal clear that it’s up to the next administration to implement this. The new guys would be handling all of its extensive recommendations for collaboration with private sector (joint public-private action). The report has its problems, yet this is likely its biggest one.

But for now, all our qualms with the report are conundrums for a quieter moment. We are on the precipice of chaos. Hucksters are selling mainly cyber solutions but also fear and uncertainty, the attackers crowd the space as they jockey to sell stolen creds for a few bucks, privacy violations heave consumers into apathy, and companies play the blame game now harder than ever. It’s a perfect storm for the selfish to advance their own interests over everyone who doesn’t get a seat at the table.

I guess that’s why the positive parts of this advisory report feel like a bitter punch. It feels slow, and it feels late. Now more than ever it feels like we’re being set up for more apathy, or worse, exploitation. It mostly feels like we should keep working on covering our own cyber-asses.

But if it makes the incoming administration think about cybersecurity a tiny bit, or as more than a tool to advance careers and screw those they disike, then I guess that little bit was worth it.

EU Threatens New Laws to Combat Online Hate Speech

European lawmakers on Sunday accused Google, Facebook, Twitter, and Microsoft of dragging their feet when it comes to combating online hate speech, and threatened to pass new laws if the companies don’t make good on their promise to remove hateful comments within 24 hours.

A report from the EU Justice Commission found that the four companies only review 40 percent of hate speech reports within 24 hours, Reuters reports. Six months ago, they agreed to a voluntary code of conduct to take action in Europe within 24 hours, and EU Justice Commissioner Vera Jourova said that shorter response times are possible.

"After 48 hours the figure is more than 80 percent. This shows that the target can realistically be achieved, but this will need much stronger efforts by the IT companies," she told Reuters. She did not set a deadline for improvements, but the Justice Commission is considering new laws that would force quicker action.

Facebook, which has also been criticized in the US in recent weeks for failing to remove fake news stories and links to hoaxes, has long pledged to corral hate speech in Europe. The company launched a "broad campaign" to encourage more civil discourse online in Germany in 2015, and announced in January that it would spend more than $1 million to fight online extremism.

But advocacy groups have criticized those efforts. In France, two organizations announced plans in May to sue Facebook, Twitter, and Google for failing to remove racist, homophobic, and other hateful posts from their platforms. A law passed in 2004 requires websites in France to remove content that is "manifestly illicit" in a timely manner if they know about it. Twitter removed just 4 percent of the offending posts during the groups’ monitoring, while Google-owned YouTube and Facebook did only slightly better.

The Justice Commission’s report found similar results in some countries, though they vary widely, Reuters reports. The removal rate of racist posts in Germany and France was above 50 percent, but just 11 percent in Austria and 4 percent in Italy.

None of the four companies immediatley responded to requests for comment on the Commission’s report.

Chrome Update Warns Users of Risky Retail Websites

Sketchy retail sites have made their way into Google s crosshairs. The latest update on its way for Google Chrome will clearly mark retail sites using out of date security protocols as being a risk to users.

The change, which will first appear in the Chrome 56 beta, will brand any website that collects passwords or credit card information while using unencrypted HTTP protocols will be labeled with as not secure directly in the address bar.

Google signaled in a blog post that the warning represented a new approach to insecure sites, which the company had previously not outed as many sites underwent the process of converting to HTTPS, which adds an additional layer of security to standard web protocol.

The threat of this public shaming in browser has been looming for some time. Google proposed a marker that would indicate when a website was non-secure back in 2014 and has experimented with various forms of the idea ever since.

Current versions of Chrome show a padlock when a website is using HTTPS and a blank white page icon when it uses standard HTTP. Sites that use HTTPS but have errors on the page display a yellow caution icon atop the padlock and sites with broken or expired HTTPS are hit with a red X atop the lock symbol.

The more direct indicator of a site s security measures should help browsers make decisions when it comes to what sites to trust. Luckily, according to Google s recent transparency report, more sites than ever are using HTTPS.

If Google s slow evolution on these types of warnings is any indication, future iterations of the search giant s browser may call even more attention to sites that haven t properly secured their service.

The new version of Chrome, complete with the not secure warning in the address bar, is available to download in its beta form for Windows, OSX and Android users though Google warns the beta is designed for developers and early adopters, and can sometimes break down completely." The public version of the update is expected in January 2017.

Twitter ’Accidentally’ Killed @ Usernames

Oops: Twitter on Thursday "accidentally" removed the @ identifier from the start of iOS users’ tweet responses.

Citing an "experiment around replies," the company gave folks a glimpse into a micro-blogging world where usernames don’t count toward character limits.

The change was quickly rolled back, amidst negative fan feedback.

"Hated it," Michelle Jones wrote in response to the Twitter Support notice.

"How dumb are you that this experiment even left the whiteboard," Sam Sabri added.

"Removing the Twitter handle makes it so much harder to identify people and properly follow a conversation," Angel Dominguez said.

Luckily for all the haters out there, Twitter said it is listening and taking stock of "helpful feedback."

The social network in May tipped changes to its username system, suggesting ditching the ".@" convention, used by many to ensure tweets directed at or citing people show up in the timelines of all followers.

But the feature was notably absent from a September revamp, in which Twitter loosened its restrictions, allowing photos, videos, GIFs, polls, and Quote Tweets to no longer count toward the 140-character limit.

"One of the biggest priorities for this year is to refine our product and make it simpler," company head Jack Dorsey said in May. "We’re focused on making Twitter a whole lot easier and faster." It remains unclear, however, whether this week’s gaffe signals an upcoming adjustment to the system, or another internal trial that will end up on the cutting room floor.

Twitter did not immediately respond to a request for comment.

Folks often forget that the popular social media site was conceived nearly a decade ago as an SMS-Web hybrid platform: The seemingly arbitrary 140-character limit corresponds to the 160-character SMS ceiling (saving an additional 20-character buffer for usernames).

Facebook s Plan to Keep Zuckerberg in Control Was Flawed, Lawsuit Says

Facebook Inc. s move to change its capital structure was tainted by secret text messages and meddling from financial advisers that pointed to a process rife with conflicts of interest, according to investor lawsuits filed in Delaware.

Late last summer, Chief Executive Mark Zuckerberg asked the board to approve a plan to create a new class of nonvoting shares that would allow him to maintain control of the company he co-founded. The board formed a three-person special committee tasked with assessing the capital plan.

Morgan Stanley, which advised Facebook, appeared to pull the strings behind the scenes by convincing the board s advisers to water down parts of the plan that would have been unfavorable to Mr. Zuckerberg, according to court documents filed by the plaintiffs.

Meanwhile, longtime Facebook director Marc Andreessen, who served on the special committee, was privately coaching Mr. Zuckerberg by text message on how to win over the other two directors, according to court documents. In one instance, Mr. Andreessen texted Mr. Zuckerberg during a March meeting of the special committee with progress reports. NOW WE RE COOKING WITH GAS, Mr. Andreessen wrote.

The capital plan was approved by the eight-member board in April.

The lawsuits allege a web of entangled interests at Facebook and the covert dealings that allowed Mr. Zuckerberg to cement his control over the company. The board showed stunning disloyalty to shareholders in approving a plan that would diminish shareholders say, investors said in court documents, which were first reported by Bloomberg.

The suits were filed in the spring, and later bundled into one by the Delaware Chancery Court. The documents were unsealed recently.

 It is clear that the process surrounding the reclassification was rife with actual, acted-upon conflicts of interest, according to the investor lawsuit, which said virtually every aspect of the process was tainted.

Representatives for Mr. Andreessen and Morgan Stanley declined to comment. Facebook is confident that the special committee engaged in a thorough and fair process to negotiate a proposal in the best interests of Facebook and its shareholders, a Facebook spokeswoman said. Mr. Zuckerberg declined to comment through a spokeswoman.

In August 2015, Mr. Zuckerberg told the board of his plans to give away 99% of his wealth to the Chan Zuckerberg Initiative LLC, a for-profit entity he created with his wife to donate to nonprofits and make private investments toward causes such as curing disease and education. He proposed a plan to overhaul Facebook s capital structure so he could keep his majority voting rights, according to court filings.

The special committee Facebook s board formed to study its options was made up of the three board members deemed by directors to have the fewest potential conflicts of interest: Mr. Andreessen, a well-known venture capitalist; Susan Desmond-Hellmann, chief executive of the Bill and Melinda Gates Foundation; and Erskine Bowles, a former White House official and president emeritus of the University of North Carolina.

Initially, the committee considered hiring Morgan Stanley as its adviser but opted not to because Mr. Bowles is a director on the bank s board, according to court documents. The committee ended up hiring Evercore Group LLC as its banker and Wachtell, Lipton, Rosen & Katz as its legal counsel. Morgan Stanley switched to providing advice to Mr. Zuckerberg s senior advisers, the lawsuit says.

Yet Morgan Stanley still was able to influence the committee s discussions in a way that favored Mr. Zuckerberg, according to the lawsuit. The bank urged Evercore and Wachtell to use as a blueprint a similar creation of nonvoting shares by Google parent Alphabet Inc. in 2014, according to the lawsuit.

Evercore removed portions of its presentation to the committee that would have facilitated robust Committee negotiations with Zuckerberg at the urging of Wachtell and Morgan Stanley, according a plaintiffs brief. Evercore scrapped its conclusion that investors would place a higher value on voting shares over nonvoting shares after a call with Morgan Stanley and Wachtell in which Morgan Stanley pushed back, court documents say.

Wachtell Lipton declined to comment. Evercore didn t respond to a request for comment.

According to court documents, Morgan Stanley Managing Director Michael Grimes said the bank landed in the right spot with the company and was happy to have volunteered advice to Mr. Zuckerberg. [T]he more we add value we could decide token fee a la goog [sic] but we wait to consider later, the bank wrote, referring to its advising of Google, according to the lawsuit.

Morgan Stanley ultimately was paid $2 million for advice, a proxy filing shows. Evercore was paid $2.5 million, according to the proxy filing. It wasn t clear what Wachtell was paid.

Throughout the special committee s deliberations, Mr. Andreessen kept in touch with Mr. Zuckerberg, assuring him that the negotiations were all intended to protect the company and you personally, according to text messages included in the court documents.

In later text messages, Mr. Andreessen conveyed that the biggest issue was Mr. Zuckerberg s desire to be able to go into government service for two years without losing control of Facebook.

Erskine is just massively uncomfortable with you getting to low economic ownership and then going off on leave with no involvement by the board and retaining control, Mr. Andreessen wrote. I m going to try to drag it over the line one more time.

The government service provision was approved and laid out in Facebook s proxy earlier this year.

Ms. Desmond-Hellmann, chair of the committee, and Mr. Bowles didn t reply to requests for comment.

On April 14, the committee agreed to approve the plan. The cat s in the bag and the bag s in the river, Mr. Andreessen wrote. Does that mean the cat s dead? Mr. Zuckerberg asked. Mission accomplished, Mr. Andreessen replied with a smiley-face emoticon.

Each director on the special committee was paid $20,000 for his or her work. The board s compensation committee, which also includes Mr. Andreessen, approved the payment, according to a proxy filing.

The capital plan was approved by shareholders in June. The outcome was no surprise, as Mr. Zuckerberg held majority voting power.

=~=~=~=